IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

George Howell, Plaintiff, v. Carrier IQ, Inc., AT&T, Inc., and Apple, Inc. Defendant.	Case No: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

George Howell ("Plaintiff"), by his undersigned counsel, for himself and all others similarly situated, hereby commences this class action suit against Defendants Carrier IQ, Inc. ("Carrier IQ" or "Defendant"), AT&T, Inc. ("AT&T"), and Apple, Inc. ("Apple") for statutory, compensatory, punitive, equitable, injunctive, and declaratory relief. Plaintiff makes the following allegations based upon personal knowledge as to his own acts, and upon information and belief, as well as upon his attorneys' investigative efforts as to Carrier IQ's actions and misconduct, and alleges as follows:

PRELIMINARY STATEMENT

1. This class action arises out of the undisclosed and unauthorized monitoring, recording, and transmission of the keystrokes, data sent and received, location, numbers dialed, message content, websites visited, encrypted web searches, and other private information of millions of mobile device users by Defendants. This information is extremely sensitive and private. AT&T and Apple Defendants acted through monitoring software designed and distributed by Carrier IQ. The software is intentionally concealed

from mobile device users. Even if consumers are aware of the software, they cannot remove or deactivate it.

2. Plaintiff brings this lawsuit on behalf of all similarly situated consumers – users of mobile devices that operate the Carrier IQ software – and alleges that Defendants' conduct violates the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* On behalf of himself and the Class, as defined below, Plaintiff seeks actual damages, statutory damages, punitive damages, disgorgement and restitution, and attorneys' fees and costs.

PARTIES

3. Individual and representative George Howell resides in and is a citizen of the State of Minnesota. Mr. Howell has owned multiple iPhones that used the Carrier IQ Software.

4. Defendant Carrier IQ, Inc. is a Delaware corporation with its principal place of business located in Mountain View, California. It is engaged in the business of developing, manufacturing, selling, and supporting diagnostic software for mobile device manufacturers and network service providers.

5. Defendant AT&T is a Delaware corporation based in Dallas, Texas. It is engaged in the business of selling wireless network service nationwide, including throughout the State of Minnesota.

6. Defendant Apple, Inc. is a California corporation based in Cupertino, California. It is engaged in the business of manufacturing and selling mobile devices nationwide, including throughout the State of Minnesota.

FACTUAL ALLEGATIONS

7. Carrier IQ designs, develops, and markets software capable of tracking, recording, and transmitting electronic data to wireless service providers or other Carrier IQ customers ("Carrier IQ Software" or "rootkit software"). Carrier IQ refers to the Carrier IQ Software as the IQ Insight Experience Manager or as the IQ Agent.

8. The Carrier IQ Software is found on over 140 million smartphones and mobile devices.

9. Wireless carriers Sprint, AT&T, and T-Mobile acknowledge that they utilize the Carrier IQ Software.[1] On December 1, 2011, Defendant AT&T confirmed that handsets on its network run Carrier IQ's Software and transmit information from it back to them. However, Defendant AT&T does not inform consumers how this information is used.

10. The Carrier IQ Software can be found on smartphones and mobile devices manufactured by HTC, Samsung, and others.[2] Apple admitted to running the Carrier IQ Software, but stated it stopped supporting it with the latest version of iOS in most products, and would remove it completely in a future software update. However, Apple confirmed that the iPhone 4 is still running Carrier IQ Software.

[1] Verizon, U.S. Cellular, C Spire, MetroPCS, and Rogers Communications deny using the Carrier IQ Software.
[2] Nokia and RIM deny installing the Carrier IQ Software on any of their mobile devices.

11. Once the Carrier IQ Software is installed on a smartphone, it surreptitiously runs in the background, capturing and logging the user's activities. The Carrier IQ Software functions by recording the user's key strokes and transmitting that data to a separate location that can be accessed by wireless service providers.

12. The Carrier IQ Software is a rootkit. A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators (consumers who own the mobile devices, including Plaintiff) by subverting standard operating system functionality or other applications.

13. The rootkit software records personal and private information, including:

a. When a user turns his or her phone on and off;

b. The phone numbers a users dials;

c. The contents of the text messages the user receives;

d. The URLs of the websites the user visits;

e. The contents of the user's online search queries; and

f. The user's location—even when the user has expressly denied permission for that information to be recorded.

14. Carrier IQ states on its website that it is the "leading provider of Mobile Service Intelligence Solutions to the Wireless Industry. As the only embedded analytics company to support millions of devices simultaneously, we give Wireless Carriers and Handset Manufacturers unprecedented insight into their customers' mobile experience."

15. Carrier IQ's website defines "Mobile Service Intelligence" as "the process of analyzing data from phones to give you a uniquely powerful insight into mobile service quality and user behavior."

16. At the direction of wireless carriers, mobile device manufacturers embedded the Carrier IQ Software in various models of smartphones and mobile devices. Consumers are not informed about the inclusion of the rootkit software on their smartphone at the time of purchase, nor at any other time.

17. In November 2011, Trevor Eckhart, a systems administrator and information technology expert in Connecticut, discovered the hidden rootkit software and posted about it (and the extensive data it captures) on his website, http://androidsecuritytest.com.

18. After Eckhart published the information he discovered on his website, Carrier IQ initially threatened him with litigation in an attempt to force him to take the information down. After public outcry – including a letter from Senator Al Franken demanding an explanation from Carrier IQ – Carrier IQ abandoned its effort to silence Eckhart.

19. In an interview with *Wired*, an online magazine, Andrew Coward, Carrier IQ's chief marketing officer, answered "probably yes" when asked whether Carrier IQ could read mobile users' text messages. Coward admitted that the data collected by the Carrier IQ Software is "a treasure trove" of "sensitive information."

20. Data logged by the rootkit software includes keystrokes. A keystroke is a character selected by the user on the user's keyboard. This means that every letter,

number, and punctuation mark that a user enters on his or her smartphone keyboard is logged by the rootkit software, including web addresses, emails, text messages, and user names and passwords (even when the website uses a secure (https) connection).

21. The Carrier IQ Software also monitors application usage.

22. Carrier IQ's website states that it "takes customer experience profiling to another level, enabling [the mobile service provider] to view experience data at any level of granularity from the entire population, to comparative groups, down to individual users, all at the touch of a button."

23. Carrier IQ advertises its software as possessing the ability to "[c]apture a vast array of experience data including screen transitions, button presses, service interactions and anomalies."

24. The Carrier IQ Software gathers the data from a person's mobile device and transmits it to either a wireless carrier's network or to other Carrier IQ facilities approved by the network.

25. The Carrier IQ Software cannot be turned off.

26. The Carrier IQ Software operates by listening for commands called "triggers." For example, a user opening an application on his or her smartphone can be a trigger for the Carrier IQ Software to record and transmit information.

27. What actions serve as triggers to the Carrier IQ Software is predetermined by Carrier IQ and the wireless service providers. At a minimum, these include every time the user: (1) presses a key on the phone; (2) changes physical locations; (3) taps the

screen; and (4) accesses a webpage. Other actions can also trigger the Carrier IQ Software.

28. Once triggered, the Carrier IQ Software records certain information. This information is then sent to another location, called the Carrier IQ Portal, where the information is stored and organized.

29. At the Carrier IQ Portal, devices are displayed by individual phone equipment ID and subscriber ID. Portal administrators can organize the information and subdivide the data sets further depending on their needs.

30. Carrier IQ's own patent for the rootkit software states that it is a "method for collecting data at a server coupled to a communications network." The patent states that the data to be collected relates "to an end user's interaction with the device," and that this interaction is "the end user's pressing of keys on the device."

31. Carrier IQ's own marketing materials further show that the rootkit software transmits personal and private data to wireless service providers. The marketing material promotes the software stating the software:

a. Is able to "capture a vast array of experience data including screen transitions, button presses, service interactions and anomalies;"

b. Allows users to see "application and device feature usage, such as camera, music, messaging, browser, and tv;" and

c. Allows users to "[i]dentify exactly how customers interact with services and which ones they use. See which content they consume, even offline."

32. The Carrier IQ Software also degrades the performance of all mobile devices in which it is installed. The software is always operating and cannot be turned off. It uses system resources, thus slowing performance and decreasing battery life. As a result, because of the Carrier IQ Software, Plaintiff and Class Members are not receiving the optimal performance of the smartphones that they purchased, which are marketed in part based on their speed, performance, and battery life.

JURISDICTION AND VENUE

33. This Court has original jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiff brings claims arising under federal law based on Defendants' violations of the Stored Communications Act, 18 U.S.C. §§ 2702 and 2707; the Wiretap Act, 18 U.S.C. § 2510 *et seq.*; and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

34. Additionally, and in the alternative, this Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A). There is minimal diversity and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

35. Venue is proper in the District of Minnesota because a substantial part of the events or omissions giving rise to the claims occurred in Minnesota, Plaintiff resides in Minnesota, and all Defendants regularly do business in and are subject to personal jurisdiction in Minnesota.

CLASS ACTION ALLEGATIONS

36. Plaintiff brings this action on behalf of himself and all others similarly situated, as members of a proposed Nationwide Plaintiff Class (the "Class") defined as follows:

> All persons residing in the United States or its territories who own or owned mobile devices on which Carrier IQ Software was installed or embedded. The Class does not include Defendants or their affiliates, officers, directors, agents, or employees.

37. The Class is so numerous that individual joinder of all its members is impracticable. While the exact number and identification of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery of Defendants, the Class is believed to number in the millions.

38. This action is brought and may properly be maintained as a class action pursuant to the provisions of Federal Rules of Civil Procedure 23(a)(1)-(4) and 23(b)(1)-(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions. Common questions of fact and law exist as to all Class members which predominate over any questions affecting only individual Class members. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any Class member, include the following:

a. Whether the Carrier IQ Software has intercepted, recorded, and retransmitted Plaintiff's personal and private information, including text messages, keystrokes, telephone numbers, and other information, without the permission or knowledge of Plaintiff;

b. Whether Defendants violated the Stored Communications Act, 18 U.S.C. § 2702;

c. Whether Defendants violated the Wiretap Act, 18 U.S.C. § 2510 *et seq.*;

d. Whether Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

e. Whether Defendants have released the content of communications to third parties and the number of times Defendants have released this information;

f. Whether Defendants' conduct invaded the Class members' privacy;

g. Whether Defendants have unjustly profited from their conduct;

h. Whether Defendants owed a duty to the Class to give notice of the existence and function of the Carrier IQ Software on Class members' mobile devices;

i. Whether Defendants owed a duty to the Class to obtain authorization from Class members to operate the Carrier IQ Software on their mobile devices;

j. Whether Plaintiff and the Class are entitled to damages, civil penalties, punitive damages, restitution, and/or injunctive or declaratory relief.

39. Plaintiff's claims are typical of the claims of the Class members. Plaintiff and other Class members must prove the same facts in order to establish the same claims, described herein, which apply to all Class members.

40. Plaintiff is an adequate representative of the Class because he is a member of the Class and his interests do not conflict with the interests of the Class members he seeks to represent. Plaintiff has retained counsel competent and experienced in the prosecution of complex class actions, and together Plaintiff and counsel intend to prosecute this action vigorously for the benefit of the Class. The interests of Class members will be fairly and adequately be protected by Plaintiff and his counsel.

41. A class action is superior to other available methods for the fair and efficient adjudication of this litigation since individual litigation of the claims of all Class members is impracticable. Even if every Class member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts, in which individual litigation of thousands of cases would proceed. Individual litigation presents a potential for inconsistent or contradictory judgments, the prospect of a race for the courthouse, and an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation increases the expense and delay to all parties and the court system in resolving the legal and factual issues common to all Class members' claims relating to the Carrier IQ Software. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

42. The various claims asserted in this action are additionally or alternatively certifiable under the provisions of Federal Rules of Civil Procedure 23(b)(1) and/or 23(b)(2) because:

a. The prosecution of separate actions by millions of individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, thus establishing incompatible standards of conduct for Defendants;

b. The prosecution of separate actions by individual Class members would also create the risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of the other Class members who are not a party to such adjudications and would substantially impair or impede the ability of

such non-party Class members to protect their interests; and

c. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making appropriate final declaratory and injunctive relief with respect to the Class as a whole.

COUNT I

Electronic Communications Privacy Act – Stored Communications Act

18 U.S.C. §§ 2702, 2707

43. Plaintiff incorporates the allegations in each above numbered paragraph.

44. The Stored Communications Act prohibits an entity providing an electronic communication service or remote computing service from knowingly divulging the contents of a communication while in electronic storage. 18 U.S.C. § 2702(a)(1)-(2).

45. Defendants provide electronic communication services to the public. 18 U.S.C. § 2510(15).

46. Defendants provide remote computing services to the public. 18 U.S.C. § 2711(2).

47. The Carrier IQ Software tracked, gathered, stored, transferred, and removed keystroke data – including data communications, phone calls, and voice messages – from Plaintiff's and Class members' mobile devices without their knowledge.

48. Defendants intentionally and knowingly divulged to third parties the contents of stored keystroke data taken from Plaintiff's and Class members' mobile devices while the keystroke data was placed in storage. Defendants knowingly divulged

the contents of Plaintiff's and Class members' communications, records and/or other information pertaining to them to third parties in violation of 18 U.S.C. § 2702(a).

49. Plaintiff and Class members have suffered actual damages as a result of Defendants' violations of 18 U.S.C. § 2702, including paying service and other fees and losing functionality and performance of their mobile devices, failing to receive the benefits of products impliedly represented to be secure with respect to personal information, and suffering the disclosure of their private information.

50. Pursuant to 18 U.S.C. § 2707, Plaintiff seeks on behalf of himself and the Class preliminary and permanent injunctive, declaratory, and equitable relief as may be appropriate; statutory damages, actual damages, and disgorgement of any profits made by Defendants as a result of this violation, in an amount no less than $1,000 per Plaintiff and Class member; punitive damages; and reasonable attorneys' fees and litigation costs.

COUNT II

Electronic Communications Privacy Act – Wiretap Act

18 U.S.C. § 2510 *et seq.*

51. Plaintiff incorporates the allegations in each above numbered paragraph.

52. The Wiretap Act, 18 U.S.C. § 2510 *et seq.*, regulates the interception and disclosure of wire, oral, and electronic communications.

53. Electronic communications are "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by" any electronic communications system that affects interstate or foreign commerce. 18 U.S.C. § 2510(12).

54. Electronic communications systems include "any computer facilities or related electronic equipment for the electronic storage of" electronic or other communications. 18 U.S.C. § 2510(14).

55. Through the Carrier IQ Software and any implementing or ancillary software exclusively controlled by Defendants, Defendants have intentionally intercepted, endeavored to intercept, and/or procured others to intercept wire, oral, and/or electronic communications without the knowledge, consent or authorization of Plaintiff or Class members, in violation of 18 U.S.C. § 2511(1)(a).

56. Through the Carrier IQ Software and any implementing or ancillary software exclusively controlled by Defendants, Defendants have intentionally disclosed and endeavored to disclose to third parties the contents of wire, oral, and electronic communications while knowing or having reason to know that information was obtained through the unlawful interception of the communications, in violation of 18 U.S.C. § 2511(1)(c).

57. Through the Carrier IQ Software and any implementing or ancillary software exclusively controlled by Defendants, Defendants have intentionally used and endeavored to use the contents of wire, oral and electronic communications while knowing or having reason to know that information was obtained through the unlawful interception of the communications, in violation of 18 U.S.C. § 2511(1)(d).

58. As a result of Defendants' violations of the Wiretap Act, Plaintiff and Class members suffered harm and injury, including the interception and transmission of private

and personal communications and the degraded performance level of their mobile devices.

59. Recovery of civil damages is authorized because Plaintiff and Class members are "person[s] whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of" the Wiretap Act. 18 U.S.C. § 2520(a).

60. Plaintiffs and the Class, pursuant to 18 U.S.C. § 2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each day of violation, actual and punitive damages, reasonable attorneys' fees and litigation costs, and Defendants' profits obtained from the violations described above. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's and Class members' remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiff to remedies, including injunctive relief, as provided by the Wiretap Act.

COUNT III

Computer Fraud and Abuse Act

18 U.S.C. § 1030

61. Plaintiff incorporates the allegations in each above numbered paragraph.

62. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), regulates fraud and related activity in connection with computers. The CFAA makes it unlawful to intentionally access a computer used for interstate commerce or communication without authorization, or to exceed authorized access to such a computer, and to thereby obtain information from a protected computer. 18 U.S.C. § 1030(a)(2)(C).

63. Plaintiff's and Class members' mobile devices are protected computers as defined by the CFAA.

64. Defendants violated the CFAA by accessing without authorization (or exceeding authorized access to) information from Plaintiff's and Class members' protected computers. 18 U.S.C. § 1030(a)(2)(C).

65. Defendants violated the CFAA by (A) knowingly causing the transmission of a program, information, code, or command, and as a result intentionally causing damage to Plaintiff's and Class members' protected computers; (B) intentionally accessing Plaintiff's and Class members' protected computers without authorization, and as a result recklessly causing damage; and (C) intentionally accessing Plaintiff's and Class members' protected computers without authorization, and as a result causing damage and loss. 18 U.S.C. § 1030(a)(5).

66. Plaintiff and Class members have suffered damages caused by Defendants' CFAA violations. Defendants' intentional actions impaired the integrity of data and information on Plaintiff's and Class members' mobile devices, including information concerning Plaintiff's and Class members' phone calls, text messages, web browsing, location and other activities through the keylogging and data transmission described above. Plaintiff and Class members have suffered loss including violation of their right to privacy and degradation of the performance of their mobile devices.

67. As a result of these injuries, Defendants' conduct has caused a loss to one or more persons during a one-year period aggregating at least $5,000 in value in real economic damages.

68. On behalf of himself and the Class, Plaintiff seeks damages pursuant to 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for judgment against Defendants as follows:

1. An Order certifying the Class and any appropriate subclasses thereof under the appropriate provisions of Federal Rule of Civil Procedure 23, and appointing Plaintiff and his counsel to represent the Class;

2. Declarations that the actions of Defendant, as set out above, are unlawful;

3. Appropriate injunctive and equitable relief;

4. Compensatory damages;

5. Punitive damages;

6. Statutory damages;

7. Restitution and/or disgorgement;

8. Costs, disbursements, expenses, and attorneys' fees;

9. Pre- and post-judgment interest, to the extent allowable; and

10. Such other and further relief as this Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a trial by jury in this case as to all issues so triable.

Dated: January 19, 2012

s/Daniel E. Gustafson
Daniel E. Gustafson (#202241)
Daniel C. Hedlund (#258337)
Joseph C. Bourne (#0389922)
GUSTAFSON GLUEK PLLC
650 Northstar East
608 Second Avenue South
Minneapolis, Minnesota 55402
Tel: (612) 333-8844
Fax: (612) 339-6622
dgustafson@gustafsongluek.com
dhedlund@gustafsongluek.com
jbourne@gustafsongluek.com

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS